UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,438	12/05/2001	Neil Y. Iwamoto	36.P325	6310

5514 7590 07/16/2007
FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
VU, THONG H	
ART UNIT	PAPER NUMBER
2616	
MAIL DATE	DELIVERY MODE
07/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/017,438	**Applicant(s)** IWAMOTO ET AL.	
	Examiner Thong H. Vu	**Art Unit** 2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *1/07*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

1. Claims 17-36 are pending.

Response to Arguments

2. Applicant's arguments filed 6/26/07 have been fully considered but they are not persuasive to overcome the prior art.

Applicant argues the prior art does not teach or suggest "access management information which identifies a feature and /or service that is available to a user"

Examiner points out the prior art taught "transferring access management data from CACS to all access controllers in access control system on an as-needed basis (= identifies a feature/service available to a user) [Rosenow, col 8 lines 10-13]

The prior art also taught a Resource Access Control Services system (RACS) [Rosenow, col 7 lines 40] are loaded authorized resource tables, access control codes and encryption keys. It's clearly the RACS server controls and provides the resources (i.e.: CACS database 60, col 12 lines 24) or services to the network devices or users [Rosenow, Fig 1] including the security features [Rosenow, col 15 lines 23-55] either available (if a valid authorized resource pair is found, col 12 line 57) or not available (if a valid authorized resource pair is not found, col 12 line 54).

Thus the rejection is sustained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 17-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Rosenow et al [Rosenow, 5,4383,596].

3. As per claim 26, Rosenow discloses A device which is accessible by a user based on access management information, comprising:

a reception unit constructed to receive, from a computer, a job and access management information for identifying a feature and/or a service of the device available to a user (i.e.: a private means or identifying a feature and/or a service of the device not available to the user), wherein the access management information is transmitted from a server to the computer [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers (or peripheral devices) on an as-needed basis, col 8 lines 10-15]; and

a controller constructed to determine, based on the received access management information, whether the user can use a feature and/or a service of the device necessary to perform the received job [Rosenow, download authorized resource tables, col 12 lines 35-38], and

constructed to perform the received job in a case that the user can use the feature and/or the service necessary to perform the received job [Rosenow, access to resources in session, col 12 lines 39-45].

4. As per claim 27 Rosenow discloses the device is a printing device and the job is a print job [Rosenow, printer, col 17 lines 35-40].

5. As per claim 28 Rosenow discloses a transmission unit constructed to transmit to the computer a message for denying the access by the user, in case that said reception unit receives the job without receiving the access management information for the user [Rosenow, disconnected in an unauthorized manner, col 7 lines 25-35; exchange message, col 13 lines 17-22].

6. As per claim 29 Rosenow discloses a transmission unit constructed to transmit to the computer a message for denying the job, in case that the user can not use the feature and/or the service necessary to perform the received job [Rosenow, disconnected in an unauthorized manner, col 7 lines 25-35; exchange message, col 13 lines 17-22].

7. As per claim 30 Rosenow discloses said reception unit receives access management information for a second user from the server without the computer, said controller determines a level of access to the device available to the second user based on the received access management information for the second user, and said controller allows the second user access to the device based on the determined level of access to the device [Rosenow, authorized resource table, col 6 line 3].

8. As per claim 31 Rosenow discloses A device which is accessible by a user based on access management information, comprising:

a reception unit constructed to receive, from a computer, a job and access management information for identifying a feature and/or a service of the device available to a user, wherein the access management information is transmitted from a server to the computer [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15]; and

a controller constructed to determine, based on the received access management information, whether the user can use a feature and/or a service of the device necessary to perform the received job [Rosenow, download authorized resource tables, col 12 lines 35-38], and

constructed to perform the received job in case that the user can use the feature and/or the service necessary to perform the received job [Rosenow, access to resources in session, col 12 lines 39-45].

9. As per claim 32 Rosenow discloses A server for use in controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, the server comprising:

a reception unit constructed to receive from a computer authentication information corresponding to a user [Rosenow, provides communication control functions required for communications between CACS and access controller, col 8 lines 35-45];

an authentication unit constructed to authenticate the user using the received authentication information [Rosenow, access management data are loaded by server into the access controller, col 7 lines 37-62]; and

a transmission unit constructed to transmit to the computer access management information for identifying a feature and/or a service of the peripheral device available to the authenticated user (or identifying a feature and/or a service of the peripheral device not available to the authenticated user), wherein the computer transmits the access management information and a job to the peripheral device [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15],

the peripheral device determines, based on the access management information, whether the user can use a feature and/or a service of the device necessary to perform the job [Rosenow, download authorized resource tables, col 12 lines 35-38], and

the peripheral device performs the job in case that the user can use the feature and/or the service necessary to perform the job [Rosenow, access to resources in session, col 12 lines 39-45].

10. As per claim 33 Rosenow discloses said reception unit receives from the peripheral device authentication information corresponding to a second user, said authentication unit authenticates the second user using the received authentication

information corresponding to the second user, said transmission unit transmits to the peripheral device access management information for identifying a feature and/or a service of the peripheral device available to the second user or identifying a feature and/or a service of the peripheral device not available to the second user, the peripheral device determines a level of access to the peripheral device available to the second user based on the access management information for the second user, and the peripheral device allows the second user access to the peripheral device based on the determined level of access to the peripheral device [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15].

11. As per claim 34 Rosenow discloses A server for use in controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, the server comprising:

a reception unit constructed to receive from a computer authentication information corresponding to a user [Rosenow, authorized users, col 3 line 10];

an authentication unit constructed to authenticate the user using the received authentication information [Rosenow, access management data are loaded by server into the access controller, col 7 lines 37-62]; and

a transmission unit constructed to transmit to the computer access management information for identifying a feature and/or a service of the peripheral device available to the authenticated user, wherein the computer transmits the access management information and a job to the peripheral device, the peripheral device determines, based on the access management information, whether the user can use a feature and/or a service of the device necessary to perform the job [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15], and

the peripheral device performs the job in case that the user can use the feature and/or the service necessary to perform the job [Rosenow, access to resources in session, col 12 lines 39-45].

12. As per claim 35 Rosenow discloses A computer for transmitting a job to a peripheral device, wherein the peripheral device is accessible by the user based on access management information, the computer comprising:

a reception unit constructed to receive from a server access management information for identifying a feature and/or a service of the peripheral device available to a user or identifying a feature and/or a service of the peripheral device not available to the user [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15]; and

a transmission unit constructed to transmit the received access management information and a job to the peripheral device, wherein the peripheral device determines whether the user can use a feature and/or a service of the peripheral device necessary to perform the job, based on the access management information [Rosenow, download authorized resource tables, col 12 lines 35-38], and

the peripheral device performs the job in case that the user can use the feature and/or the service necessary to perform the job [Rosenow, access to resources in session, col 12 lines 39-45].

13. As per claim 36 Rosenow discloses a second transmission unit constructed to transmit to the server authentication information corresponding to the user, wherein the server authenticates the user using the authentication information and transmits the access management information for the authenticated user to the computer [Rosenow, a RACS server, col 7 lines 37-62].

14. As per claim 17 Rosenow discloses A method for controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, the method comprising the steps of:

receiving, at a computer, from a server access management information for identifying a feature and/or a service of the peripheral device available to a user or identifying a feature and/or a service of the peripheral device not available to the user [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15];

receiving, at the peripheral device, the access management information and a job from the computer [Rosenow, encryption keys or access management data are loaded by server into the access controller, col 7 lines 37-62];

determining, at the peripheral device, whether the user can use a feature and/or a service of the peripheral device necessary to perform the received job, based on the received access management information [Rosenow, download authorized resource tables, col 12 lines 35-38]; and

performing, at the peripheral device, the received job in a case that the user can use the feature and/or the service necessary to perform the received job [Rosenow, access to resources in session, col 12 lines 39-45].

15. As per claim 18 Rosenow discloses receiving, at the server, authentication information corresponding to the user from the computer; and authenticating, at the server, the user based on the received authentication information, wherein the server transmits the access management information to the computer after the server authenticates the user [Rosenow, authorized users, col 3 line 10].

16. As per claim 19 Rosenow discloses the authentication information includes a user name and/or a password [Rosenow, user profile, col 7 lines 1-20].

17. As per claim 20 Rosenow discloses transmitting, at the peripheral device, to the computer a message for denying the access by the user, in case that the peripheral

device receives the job without receiving the access management information for the user [Rosenow, disconnected in an unauthorized manner, col 7 lines 25-35].

18. As per claim 21 Rosenow discloses transmitting, at the peripheral device, to the computer a message for denying the job, in case that the user can not use the feature and/or the service necessary to perform the received job [Rosenow, disconnected in an unauthorized manner, col 7 lines 25-35].

19. As per claim 22 Rosenow discloses transmitting, at the computer, to the server a request for the access management information, wherein the request identifies the user and the peripheral device, wherein the computer receives the access management information corresponding to the user and the peripheral device [Rosenow, authorized users, col 3 line 10].

20. As per claim 23 Rosenow discloses receiving, at the peripheral device, access management information for a second user from the server without the computer; determining, at the peripheral device, a level of access to the peripheral device available to the second user based on the received access management information for the second user; and allowing, at the peripheral device, the second user access to the peripheral device based on the determined level of access to the peripheral device [Rosenow, providing a private and dedicated means of transferring access management data from CACS to all access controllers on an as-needed basis, col 8 lines 10-15].

21. As per claim 24 Rosenow discloses receiving, at the server, authentication information corresponding to the second user from the peripheral device; and authenticating, at the server, the second user based on the received authentication information, wherein the server transmits the access management information for the second user to the peripheral device after the server authenticates the second user [Rosenow, authorized users, col 3 line 10].

22. As per claim 25, Rosenow discloses A method for controlling access to a peripheral device by a user, wherein the peripheral device is accessible by the user based on access management information, the method comprising the steps of:

receiving, at a computer, from a server access management information for identifying a feature and/or a service of the peripheral device available to a user [Rosenow, a RACS server, col 7 lines 37-62];

receiving, at the peripheral device, the access management information and a job from the computer [Rosenow, encryption keys or access management data are loaded by server into the access controller, col 7 lines 37-62];

determining, at the peripheral device (i.e.: access controller device), whether the user can use a feature and/or a service of the peripheral device necessary to perform the received job, based on the received access management information [Rosenow, download authorized resource tables, col 12 lines 35-38]; and

performing, at the peripheral device, the received job in a case that the user can use the feature and/or the service necessary to perform the received job [Rosenow, access to resources in session, col 12 lines 39-45].

23. Claims 25-36 contain the identical limitations set forth in claims 17-24. Therefore claims 25-36 are rejected for the same rationale set forth in claims 17-24.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner *Thong Vu*, whose telephone number is (571)-272-3904. The examiner can normally be reached on Monday-Thursday from 6:00AM- 3:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, *Lynn Feild*, can be reached at (571) 272-2092. The fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thong Vu
Primary Examiner

THONG VU
PRIMARY PATENT EXAMINER